| | |
|---|---|
| | Policy |
| | Phil Rogers, Head of Information Security & IT Compliance |
| | Draft |
| | August 2023 |
| | Executive Team |

## 1. Introduction

This End User Device

- Personally owned devices must not be used for activities that require administrative access to IT Systems.
- Minimise the amount of University data stored locally on the device and do not access or store any data classified as Confidential or above.
- Access University information assets via the University's remote access services wherever possible rather than transferring the information directly to a device. See section 3.2 of LSHTM's Bring Your Own Device Policy for more information: https://www.lshtm.ac.uk/sites/default/files/bring-your-own-device-policy.pdf
- Consider switching on device tracking/location services in the event of device theft or loss.
- If a personally owned device needs to be repaired, ensure that the company you use is subject to a contractual agreement which guarantees the secure handling of any data stored on the device.
- Devices must be disposed of securely, including the removal of University data before disposal, in accordance with LSHTM's Data Classification and Handling Policy https://www.lshtm.ac.uk/sites/default/files/data-classification-and-handling-policy.pdf

### 3.2 LSHTM Owned Devices

LSHTM

Hybrid/Remote Working Guidance:
https://lshtm.sharepoint.com/sites/intranet-it-services/SitePages/Hybrid-and-Remote-Working.aspx

Password Guidance:
https://lshtm.topdesk.net/tas/public/ssp/content/detail/knowledgeitem?unid=5516d7ab6d3044a2850c5fdc0e58a1c3

Data and International Travel Guidance